I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on December 3, 2008.

TOWNSEND and TOWNSEND and CREW LLP

By: /Kay Barclay/
Kay Barclay

PATENT
Attorney Docket No. 020375-043300US
Client Ref. No. 030610191210

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Justin Monk, et al.

Application No.: 10/690,394

Filed: October 20, 2003

For: SYSTEMS AND METHODS FOR FRAUD MANAGEMENT IN RELATION TO STORED VALUE CARDS

Confirmation No. 3753

Examiner: Thu Thao Havan

Technology Center/Art Unit: 3693

APPELLANTS' BRIEF UNDER 37 CFR §41.37

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Further to the Notice of Appeal mailed on November 4, 2008 for the above-referenced application, Appellants submit this Brief on Appeal.

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST 3

2. RELATED APPEALS AND INTERFERENCES 3

3. STATUS OF CLAIMS 3

4. STATUS OF AMENDMENTS 3

5. SUMMARY OF CLAIMED SUBJECT MATTER 3

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL 7

7. ARGUMENT 7

8. CONCLUSION 11

9. CLAIMS APPENDIX 12

10. EVIDENCE APPENDIX 17

11. RELATED PROCEEDINGS APPENDIX 18

1. REAL PARTY IN INTEREST

The real party in interest is First Data Corporation.

2. RELATED APPEALS AND INTERFERENCES

No other appeals or interferences are known which will directly affect, are directly affected by, or have a bearing on the Board decision in this appeal.

3. STATUS OF CLAIMS

Claims 1-20 were originally filed in the application on October 20, 2003, and claims 1, 6, 15, 16, and 19 were amended June 29, 2005. Claims 3 and 7 were canceled and claim 21 was added June 29, 2005. Claims 1 and 6 were further amended March 30, 2006. Claim 8 was amended April 8, 2008.

All of the remaining claims 1-2, 4-6, 8-21 stand rejected and are the subject of this appeal.

Claims 3 and 7 have been canceled.

No claims have been withdrawn.

No claims stand allowed.

4. STATUS OF AMENDMENTS

An amendment was submitted on September 10, 2008, after the Final Office Action. This after-final amendment did not amend, cancel or withdraw any claims. The amendment was entered, and an Advisory Action mailed October 14, 2008 maintained the rejections given for claims 1-2, 4-6, and 8-21 in the Final Office Action.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the invention relate to fraud management systems and methods to prevent the laundering of stolen funds into stored value products like gift cards (Specification page 1 lines 12-16). Thieves who traffic in stolen credit card accounts and bank accounts have long understood that they quickly have to convert the funds in these accounts into more

anonymous forms of currency such as cash, gold, jewelry, *etc.* More recently, they have exploited the relative anonymity of stored value products, which may be purchased in merchant stores and over the Internet without having to provide a name, address, telephone number, or other type of personal identification. Thus, conversion of stolen funds into stored value products is becoming an increasing problem for consumers, merchants and law enforcement.

Thieves also like stored value products because they can purchase them in a way that circumvents conventional methods of fraud detection based on a payment account's "transaction velocity." A transaction velocity may be determined from the number of transactions being conducted with the account over a predefined period, the amount transacted over the period, *etc.* (Specification page 10 lines 13-28). Accounts that have a suspiciously high transaction velocity may be flagged as potentially being involved in fraudulent transactions (Specification page 10 line 29 to page 11 line 4). To avoid raising suspicion, the thieves spread out their fraudulent transactions among several stored value products issued by different issuers. Because the issuers have little information about who is using the card, and do not communicate with each other, the transaction velocity for each stored value card appears normal.

Embodiments of the invention address this security weakness in transaction velocity measurements with systems that have analysis engines that can determine a transaction velocity from transactions made with different stored value products from different issuers (Specification page 2 lines 2-10). This requirement is fundamental to addressing a security weakness in transaction velocity measurements when fraudulent transactions are spread out over multiple stored value products from multiple issuers. Embodiments of the invention include systems and methods for calculating a transaction velocity from transactions using stored value products from different issuers to close this security loophole (Specification page 3 lines 11-12).

Independent claim 1

Independent claim 1 recites an account acquisition fraud management system that includes a second analysis engine that is "operable to recognize a common load source account to associate the transactions and determine a transaction velocity from the first and second transaction information" (Specification page 10 lines 18-24). The first transaction information is

"about a first transaction with the first stored value product" and the second transaction information is "about a second transaction with the second stored value product," where the second stored value product is "from a different issuer than an issuer of the first stored value product" (Specification page 2 lines 2-10). Thus, claim 1 addresses the security weakness described above by determining a transaction velocity from transactions on different stored value products from different issuers.

The system in claim 1 also includes a cross monitor that is operable to accept the first transaction information from a first analysis engine about the first transaction with the first stored value product, and the second transaction information from the second analysis engine about a second transaction with the second stored value product issued by a different issuer than the first stored value product (Specification page 7 lines 17-24). The cross monitor provides the first transaction information to the second analysis engine, which determines a transaction velocity from both the first and second transaction information after recognizing that there is a common load source account to associate the transactions (Specification page 10 lines 15-24). If the second analysis engine finds that the transaction velocity exceeds a velocity threshold, it can stall the second transaction (Specification page 11 lines 15-17). An overview of an embodiment of the system is shown in Fig. 1.

Independent claim 6

Independent claim 6 describes a method for detecting fraud in relation to stored value products, where the method includes the steps of receiving a first suspicious activity indication from a first issuer analysis engine that is operable to monitor the activities of a first plurality of stored value products, and receiving a second suspicious activity indication from a second issuer analysis engine that is operable to monitor the activities of a second plurality of stored value products (Specification page2 line 30 to page 3 line 7). The first and second plurality of stored value products are associated with different issuers (Specification page 2 line 31 to page 3 line 2), and the method addresses the security weakness described above by calculating a transaction velocity for a current transaction based the transaction and the suspicious activity indications from the different first and second issuers (Specification page 3

lines 5-12). Thus, claim 6 also addresses the security weakness in determining a transaction velocity by using information associated with at least two different stored value product issuers to calculate the transaction velocity.

The method in claim 6 also includes the step of associating the first suspicious activity indication and the second suspicious activity indication in a global negative file based on a common load source account used to load value on the plurality of the first and the second stored value products (Specification page 3 lines 2-12). When an activity request that includes transaction information about a current transaction is received from the first issuer analysis engine, the global negative file is accessed to identify the common load source account based at least in part on the transaction information (Specification page 3 lines 5-11). The method further includes associating the transaction with the first and second suspicious activity indications and calculating the transaction velocity based on the suspicious activity indications as well as the transaction (Specification page 3 lines 8-12). Using the calculated transaction velocity, the method calls for providing a response indicating whether the current transaction exceeds a velocity threshold (Specification page 10 line 29 to page 11 line 4). An overview of an embodiment of the method is shown generally in Figs. 2A-B.

Independent claim 16

Independent claim 16 describes a system for suppressing fraudulent activity in relation to account acquisition (Specification page 1 line 29 to page 2 line 1). The system addresses the security weakness in determining a transaction velocity by having a cross monitor that is operable to associate information from different monitors associated with different issuers with a transaction, and using this information to determine a transaction velocity for the transaction (Specification page 2 lines 1-14). Thus, information from different issuers is combined to determine a transaction velocity, thwarting attempts to reduce a calculated transaction velocity by spreading around transactions on stored value products associated with different issuers.

The system of claim 16 also includes first load and enrollment monitors associated with the first issuer and second load and enrollment monitors associated with the second issuer

(Specification page 3 lines 13-24). The cross monitor uses common load source account information to associate information from the first load or enrollment monitor and the second load or enrollment monitor with the transaction, and then use this information to determine the transaction velocity for the transaction (Specification page 3 lines 17-24). The cross monitor is also operable to communicate the determined transaction velocity to both the first and second issuers (Specification page 3 lines 19-21).

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 2, 4-6 and 8-21 are unpatentable under 35 U.S.C. § 102(e) over U.S. Patent Appl. No. 2003/0187783 of Arthus et al. ("Arthus"). Pages 2 through 6 of the Office Action mailed January 1, 2008, and the Advisory Action mailed October 14, 2008 describe the Examiner's position on this issue.

7. ARGUMENT

The Final Office Action mailed July 10, 2008, has rejected all pending claims 1, 2, 4-6 and 8-21 under 35 U.S.C. 102(e) as being allegedly anticipated by U.S. Pat. App. Pub. No. 2003/0187783 of Arthus et al. ("Arthus"). Applicants respectfully traverse because Arthus does not disclose, either expressly or inherently, each and every element of Applicants' claims.

Applicants' invention is directed to detecting *account acquisition fraud.* As is explained in Applicants' specification, account acquisition is the opening of an account. (Specification paragraph [0005]). The present invention aims to detect a kind of fraud wherein a person or entity opens several stored value accounts that are spread across multiple issuers and that are funded from the same *load source.* A load source is the bank or other account used by the person opening the account to provide the funds that are loaded into the stored value accounts. (Specification paragraph [0036]). A large number of stored value accounts being opened with payment from a single load source may indicate that fraud is occurring. However, if the accounts are spread among multiple issuers, no single issuer may detect any unusual activity. The invention provides a way for the issuers to share information cooperatively, so that this kind of fraud may be detected.

Claims 1, 2, 4, and 5

In the language of claim 1, a *first analysis engine is associated with a first stored value product.* A *second analysis engine is associated with a second stored value product from a different issuer than an issuer of the first stored value product.* As is shown in Figure 1, these analysis engines may be associated with the separate issuers.

A *cross monitor is operable to accept a first transaction information from the first analysis engine about a first transaction with the first stored value product and a second transaction information from the second analysis engine about a second transaction with the second stored value product, wherein the first transaction information is provided from the cross monitor to the second analysis engine.* That is, the cross monitor passes transaction information between the two analysis engines. This cross monitor makes the connection between the two issuers.

The second analysis engine can then *recognize a common load source account to associate the transactions and determine a transaction velocity from the first and second transaction information.* That is, the second analysis engine, associated with one of the issuers, recognizes that multiple stored value accounts have been opened and funded from the same load source. This can be recognized even if the multiple accounts were opened at multiple issuers, because of the information transfer performed by the cross monitor. The second analysis engine then determines a *transaction velocity*, which is an indication of the amount of activity associated with an account. (Specification paragraph [0029]).

Finally, the method includes *stalling the second transaction when the transaction velocity exceeds a velocity threshold.* This stalling permits further analysis of the transaction. (Specification paragraph [0042]).

In summary, in the present invention, issuers cooperate to detect fraud perpetrated by persons opening accounts.

Claim 1 of the present application recites

1. *An account acquisition fraud management system, the account acquisition fraud management system comprising:*
   a first analysis engine, wherein the first analysis engine is associated with a first stored value product;
   a second analysis engine, wherein the second analysis engine is associated with ***a second stored value product from a different issuer than an issuer of the first stored value product****; and*
   a cross monitor*, wherein the cross monitor is operable to accept a first transaction information from the first analysis engine about a first transaction with the first stored value product and a second transaction information from the second analysis engine about a second transaction with the second stored value product, wherein the first transaction information is provided from the cross monitor to the second analysis engine; and*
   wherein the second analysis engine is ***operable to recognize a common load source account*** *to associate the transactions and determine a transaction velocity from the first and second transaction information,* ***and stalling the second transaction when the transaction velocity exceeds a velocity threshold****.*

By contrast, Arthus describes a system for detecting fraud perpetrated by merchants, not account holders. (See Arthus paragraph [0005]). While the system of Arthus monitors multiple merchants, Arthus does not describe any cross monitoring. That is, Arthus gives no indication that activities of one merchant or account can reflect on another.

At least the portions of claim 1 highlighted above are missing from Arthus.

In support of the rejection, the Final Office Action cites various portions of Arthus, but the cited portions are for the most part unrelated to the claim terms for which they are cited. For example, the Final Office Action cites paragraphs [0057], [0008], [0030], and [0049] as disclosing *a second analysis engine, wherein the second analysis engine is associated with a second stored value* ***product from a different issuer than an issuer of the first stored value product****,* but the cited paragraphs do not support the rejection. Paragraphs [0057] and [0049] seem unrelated to this claim element. Paragraphs [0008] and [0030] do relate to monitoring of multiple merchants, but not monitoring of accounts with different ***issuers***. The Final Office Action also erroneously equates merchants with issuers. (Final Office Action p. 2).

In another example, the Office Action cites paragraph [0042] of Arthus for disclosing *stalling the second transaction when the transaction velocity exceeds a velocity threshold.* However, Arthus' paragraph [0042] describes gathering various kinds of transaction information for "later evaluation". This paragraph does not even suggest any analysis of whether the transaction information indicates that any *velocity threshold* is reached, and certainly does not disclose *stalling* a transaction. The fact that Arthus gathers data for "later evaluation" indicates that Arthus lacks the real-time aspect of stalling a transaction in progress.

In another example, the Office Action cites Arthus' paragraphs [0057], [0030], [0042], and [0049] as disclosing a *cross monitor* that passes information between two analysis engines. Paragraph [0057] describes various reports that Arthus' system can produce, and is unrelated to any cross monitoring. Paragraph [0030] indicates that a merchant's activities can be monitored, but completely lacks any suggestion of a *cross monitor* that passes information between analysis engines. Paragraph [0042] describes collection of transaction information, but does not indicate that the transaction information is shared among issuers. Paragraph [0049] describes part of the user interface of Arthus' system. None of the cited passages even suggests a cross monitor *operable to accept a first transaction information from the first analysis engine about a first transaction with the first stored value product and a second transaction information from the second analysis engine about a second transaction with the second stored value product, wherein the first transaction information is provided from the cross monitor to the second analysis engine.*

In the discussion of claim 1, the Final Office Action completely ignores the limitation that *the second analysis engine is operable to recognize a common load source account.* A common load source also appears in claim 4, and the Final Office Action cites paragraph [0012] of Arthus in relation to claim 4. Arthus' paragraph [0012] does not relate to the load source of a stored value account.

Neither the cited passages nor any other part of Arthus discloses these claim elements, and claim 1 and is not anticipated by Arthus. Claims 2, 4, and 5 depend from claim 1 and add further limitations, and are therefore also not anticipated by Arthus for at least this reason, as well as for the novel elements they recite.

Claims 6 and 8-15

Independent claim 6 is a method claim that describes cross monitoring and associating suspicious behavior based on a common load source account. As is explained above with respect to claim 1, at least these elements of claim 6 are missing from Arthus, and claim 6 and its dependent claims are not anticipated by Arthus.

Claims 16-21

Independent claim 16 also recites a *cross monitor* that associates information from separate issuers based on *load source account information*. As is explained above with respect to claim 1, these aspects are missing from Arthus. Claim 16 and its dependent claims are not anticipated by Arthus.

8. CONCLUSION

For these reasons, it is respectfully submitted that the rejection should be reversed.

Respectfully submitted,

David W. Boyd

David W. Boyd
Reg. No. 50,335

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300

61702866 v1

9. CLAIMS APPENDIX

1. An account acquisition fraud management system, the account acquisition fraud management system comprising:

a first analysis engine, wherein the first analysis engine is associated with a first stored value product;

a second analysis engine, wherein the second analysis engine is associated with a second stored value product from a different issuer than an issuer of the first stored value product; and

a cross monitor, wherein the cross monitor is operable to accept a first transaction information from the first analysis engine about a first transaction with the first stored value product and a second transaction information from the second analysis engine about a second transaction with the second stored value product, wherein the first transaction information is provided from the cross monitor to the second analysis engine; and

wherein the second analysis engine is operable to recognize a common load source account to associate the transactions and determine a transaction velocity from the first and second transaction information, and stalling the second transaction when the transaction velocity exceeds a velocity threshold.

2. The system of claim 1, wherein the system further comprises:

a computer readable medium accessible to the cross monitor, wherein the computer readable medium includes the first transaction information and the second transaction information.

3. (Cancelled)

4. The system of claim 1, wherein the first transaction information and the second transaction information are selected from a group consisting of:

a physical address;

a telephone number;

a virtual address; and

a load source.

5. The system of claim 1, wherein the cross monitor is further operable to maintain the first transaction information is a queue associated with an issuer of the second stored value card product.

6. A method for detecting fraud in relation to stored value products, the method comprising:

receiving a first suspicious activity indication from a first issuer analysis engine, wherein the first issuer analysis engine is operable to monitor activities occurring in relation to a first plurality of stored value products associated with the first issuer;

receiving a second suspicious activity indication from a second issuer analysis engine, wherein the second issuer analysis engine is operable to monitor activities occurring in relation to a second plurality of stored value products associated with a second issuer different from the first issuer;

associating the first suspicious activity indication and the second suspicious activity indication in a global negative file based on a common load source account used load value on the plurality of the first and the second stored value products;

receiving an activity request from the first issuer analysis engine, wherein the request includes a transaction information about a current transaction with one of the first plurality of stored value products associated with the first issuer;

based at least in part on the transaction information, accessing the global negative file, wherein the transaction information includes the identity of the common load source account;

associating the current transaction with the first suspicious activity indication and the second suspicious activity indication and calculating a transaction velocity based on the transaction information, and the first and second suspicious activity indications in the global negative file; and

providing a response, wherein the response indicates whether the current transaction exceeds a velocity threshold.

7. (Cancelled).

8. The method of claim 6, wherein the transaction information is selected from a group consisting of:

a physical address;

a telephone number;

a virtual address; and

a load source.

9. The method of claim 6, wherein the transaction information is a physical address.

10. The method of claim 6, wherein the transaction information is a telephone number.

11. The method of claim 6, wherein the transaction information is a virtual address.

12. The method of claim 6, wherein the response is maintained in a queue associated with the first issuer.

13. The method of claim 12, wherein the response includes at least two of the following:

a date of the suspicious behavior;

a funding account number;

a denial reason;

a review status; and

a reviewer note.

14. The method of claim 12, wherein the response includes an indication of related accounts.

15. The method of claim 6, wherein the response is a first response associated with a first account, wherein the global negative file includes information about a second account having one or more items of the transaction information in common with the first account, and wherein the method further comprises:

identifying the second account using the transaction information, and providing a second response to the second issuer associated with the second account.

16. A system for suppressing fraudulent activity in relation to account acquisition, the system comprising:

a first load monitor associated with a first issuer;

a second load monitor associated with a second issuer;

a first enrollment monitor associated with the first issuer;

a second enrollment monitor associated with the second issuer; and

a cross monitor, wherein the cross monitor is operable to associate information from the first load monitor or first enrollment monitor, and the second load monitor or second enrollment monitor with a transaction using a first stored value product using common load source account information, and wherein the cross monitor is operable to determine a transaction velocity for the transaction using the information, and communicate the transaction velocity to both the first issuer and the second issuer.

17. The system of claim 16, wherein a request to load value on a stored value product associated with the first issuer is processed at least in part by the first load monitor.

18. The system of claim 17, wherein the first load monitor is operable to apply a velocity check on a load request.

19. The system of claim 16, wherein the first load monitor is further operable to compare the transaction velocity with a predefined velocity limit.

20. The system of claim 19, wherein the first load monitor is operable to provide a detected suspicious activity to the cross monitor.

21. The system of claim 20, wherein the detected suspicious activity is that the transaction velocity has exceeded the predefined velocity limit.

10. EVIDENCE APPENDIX

None.

11. RELATED PROCEEDINGS APPENDIX

None.